GIBSON, DUNN & CRUTCHER LLP
Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Martie Kutscher (SBN 302650)
mkutscherclark@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

GIBSON, DUNN & CRUTCHER LLP
Deborah Stein (SBN 224570)
dstein@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Attorneys for Defendant Facebook, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

DECLARATION OF BRIAN KENNELLY Q.C. IN SUPPORT OF DEFENDANT FACEBOOK, INC.'S OPPOSITION TO PLAINTIFFS' MOTION FOR LEAVE TO FILE SECOND AMENDED CONSOLIDATED COMPLAINT

Judge: Hon. Vince Chhabria
Courtroom 4, 17th Floor
Hearing Date: June 4th, 2020
Hearing Time: 2:00 p.m.

DECLARATION OF BRIAN KENNELLY Q.C.

Under 28 U.S.C. § 1746 and Federal Rule of Civil Procedure 44.1, I declare as follows.

1. I am a dual qualified barrister. I was called to the Bar of England & Wales in 1999 and the Bar of Ireland in 2008, and was appointed a Queens Counsel in 2016. I specialise in EU, competition, commercial, public and regulatory law, and am recognised as a leading barrister in these areas. I attach my current practising certificates issued by the Bar Council in England and the Law Library in Ireland, marked as Exhibit A.

A. SUMMARY

2. I am asked to provide an Opinion addressing a number of issues that arise under English and Irish law, that are relevant to a multi-district consumer class action that has been brought against Facebook Inc. in the United States District Court, Northern District of California ("the MDL"). The MDL arises out of events relating to Cambridge Analytica. The principal allegations in that litigation are that Facebook Inc. (i) made sensitive user information available to countless companies and individuals without the consent of the users; and (ii) failed to prevent those same companies and individuals from selling or otherwise misusing the information.[1] Claims have been brought on various legal bases, including the Californian tort of public disclosure of private facts[2]; the Californian tort of intrusion into private affairs, and the constitutional right to privacy[3]; the Californian torts of negligence and gross negligence;[4] deceit by concealment[5]; breach of contract, breach of the implied covenant of good faith and fair dealing and unjust enrichment[6]; and the federal Video Privacy Protection Act and Stored Communications Act.[7]

---

[1] See *In Re: Facebook Inc., Consumer Privacy User Profile Litigation* (MDL No. 2843, Case No. 18-md-2843-VC), Pre-Trial Order No. 20 ("Pre-Trial Order"), p.1.
[2] Pre-Trial Order, pp.30-31.
[3] Pre-Trial Order, pp.32-33.
[4] Pre-Trial Order, pp.35-38.
[5] Pre-Trial Order, p.30.
[6] Pre-Trial Order, pp.38-41.
[7] Pre-Trial Order, pp.33-35.

3. The following additional background is relevant to this Opinion:

(1) The original Consolidated Complaint, filed on 21 September 2018, defined the class as "*all Facebook users in the United States and in the United Kingdom whose content and information, generated when they were eighteen years of age or older, was collected by Facebook and published and/or disclosed to third parties without their authorization or consent from January 1, 2007 to the present*" (at §437) ("the Proposed Class"). The Consolidated Complaint included Bridget Peters, a UK citizen and resident of Hampshire, England, as a named representative plaintiff (§§87-88).

(2) The same plaintiff was named in the First Amended Consolidated Complaint, filed on 22 February 2019 (§§60-67).

(3) On 20 February 2020, Facebook Inc. was informed that Bridget Peters would be unable to continue as a named plaintiff.

(4) On 14 April 2020, the plaintiffs applied for permission to file a Second Amended Consolidated Complaint that removed Bridget Peters, and added two new United Kingdom plaintiffs: (i) Naomi Butler, a UK citizen and resident of Liverpool in England (§§77-84); and (ii) Peter Christley, a UK citizen and resident of Rhyl Denbighshire in Wales (§§94-101). The Proposed Class remains the same (§798).

(5) Facebook Inc. is opposing the motion to amend to the extent that it includes UK plaintiffs in the proposed class.

4. Against that background, I have been asked the following:

(1) To outline the extent to which English and/or Irish law protects individual privacy generally, and data privacy in particular. In particular, I have been asked to outline, without limitation, the following sources of protection, and to provide an overview of their scope and content:

(i) data privacy protection subsequent to the implementation of Regulation (EU) 2016/679 ("the GDPR");

(ii) data privacy protection prior to the implementation of the GDPR;

(iii) the equitable doctrine of breach of confidence;

(iv) the tort of misuse of private information (in England);

(v) the constitutional right to privacy (in Ireland);

(vi) and Article 8 of the European Convention on Human Rights ("ECHR").

(2) To consider the effect of the jurisdiction clause contained within Facebook's Terms of Service applicable to UK users. I am instructed that the UK plaintiffs' contractual counterparty and the data controller in respect of their data on the Facebook platform was at all material times Facebook Ireland Limited ("Facebook Ireland"). Any claim for breach of the Terms of Service or the duties of a data controller under the data protection legislation would be against Facebook Ireland, not Facebook, Inc.

(3) To describe the approach that the English courts and Irish courts would adopt in applying the doctrine of *res judicata* and abuse of process in circumstances where:

(i) Facebook users based in the UK seek to litigate issues already determined in the MDL against Facebook, Inc., in circumstances where those users are *not* part of the class certified in the MDL;

(ii) Facebook users based in the UK seek to litigate issues already determined in the MDL against Facebook, Inc., in circumstances where those users *are* part of the class certified in the MDL.

(4) To describe the procedures that would be available for the US Court, in the event that the Proposed Class was certified, to obtain evidence located in the UK, including through the applicable standard for the disclosure of documentary evidence, and any procedural limitations of the Hague Convention process.

(5) To describe the procedures, in the event that the Proposed Class was certified, for giving UK class members notice of the MDL proceedings under the Hague Service Convention, including any practical difficulties associated with using the Hague Service Convention.

5. I address each of these issues in turn.

B. THE PROTECTION OF INDIVIDUAL PRIVACY AND DATA PROTECTION IN ENGLAND AND IRELAND

6. There is no single overarching right to privacy or data protection under the English or Irish common law. The majority of the rights are provided under EU and domestic legislation governing data protection. These are complemented by common law and equity, which has been influenced, in particular, by Article 8 ECHR.[8] In Ireland, additional protection is afforded under Bunreacht na hÉireann ("the Constitution"). Together, these legislative, common law, equitable and constitutional protections provide a comprehensive and robust framework to protect data and other private information from unwarranted intrusion and dissemination. The discussion that follows provides an outline of the scope and content of the relevant sources of protection.

(1) Data privacy protection following the implementation of the GDPR

The GDPR

7. The starting point for both England and Ireland is the GDPR. Adopted in April 2016, and applicable from 25 May 2018, the GDPR is the centerpiece of the EU regulatory framework for

[8] Article 8 ECHR provides "*(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*" Both the United Kingdom and Ireland are party to the ECHR, and have domestically incorporated the provisions by, respectively, the Human Rights Act 1998 and the European Convention on Human Rights Act 2003.

the protection of personal data. As an EU Regulation, the GDPR has direct effect, and is enforceable in both the UK and Ireland without further implementation.

8. The key features of the GDPR can be summarised as follows:

(1) The GDPR applies to the processing of "*personal data*" (Article 1).

(2) "*Personal data*" relates to an "*identified or identifiable natural person*" (a "*data subject*") (Article 4(1)). An identifiable natural person is "*one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or society identity of that natural person*" (Article 4(1)).

(3) "*Controller*" means "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*" (Article 4(7)).

(4) "*Processor*" means "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*" (Article 4(8)).

(5) Article 5 sets out six key principles relevant to the processing of personal data, which a data controller shall be responsible for. These principles provide that personal data shall be: (a) processed lawfully, fairly and in a transparent manner; (b) only be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes; (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (d) accurate, and where necessary, kept up to date; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (f) processed in a manner that ensures appropriate security of the personal data.

(6) Article 6(1) provides that the processing of personal data will only be lawful if one of the following legal bases exists:

(i) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(ii) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(iii) processing is necessary for compliance with a legal obligation to which the controller is subject;

(iv) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(v) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(vi) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(7) Article 9(1) prohibits the processing of "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*", unless one of the exceptions in Article 9(2) apply. Member States are permitted to introduce further conditions, including limitations, with regard to the processing of "*genetic data, biometric data or data concerning health*" (Article (9(4)).

(8) "*Data subjects*" (i.e. individuals) are afforded a range of rights in Chapter 3 of the GDPR. These include:

(i) the right to be informed about use of the data (Articles 13 and 14);

(ii) the right of access (Article 15);

(iii) the right of rectification (Article 16);

(iv) the right to erasure (also known as the "*right to be forgotten*") (Article 17);

(v) the right to restrict processing (Article 18);

(vi) the right to data portability (Article 20);

(vii) the right to object to the processing of data (Article 21); and

(viii) the right not to be subject to automated decision-making and profiling (Article 22).

(9) The GDPR allows Member States to introduce legislative measures that provide derogations to the rights outlined above,[9] in certain circumstances (Article 23). However, any derogation must respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society to safeguard the interests listed in Article 23 (e.g. national security, defence, prevention of crime). In addition, Article 85 permits certain exemptions for reasons relating to freedom of expression and Article 89 permits exemptions for reasons relating to scientific or historical research purposes, statistical purposes and archiving purposes.

9. Chapter 8 of the GDPR, titled "*Remedies, liabilities and penalties*", is particularly relevant for the purposes of this Opinion.

10. All data subjects have a right to lodge a complaint with a supervisory authority (Article 77), and to an effective remedy against that supervisory authority if it does not handle a complaint,

[9] It also allows for derogations to the data processing principles set out under Article 5, insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, and Article 35, which concerns the obligation to communicate personal data breaches to data subjects.

or does not inform the data subject within three months on the progress or outcome of a complaint (Article 78).

11. All data subjects also have a right to *"an effective judicial remedy where he or she considers that his or her rights under the [GDPR] have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation"* (Article 79(1)). This is underpinned by the right to an effective remedy protected under Article 47 of the Charter of Fundamental Rights of the European Union ("EU Charter"). Proceedings against a controller or processor may be brought either *"before the courts of the Member State where the controller or processor has an establishment"* or *"before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers"* (Article 79(2)). This right is without prejudice to any available administrative or non-judicial remedies, including the right to lodge a complaint to a supervisory authority pursuant to Article 77.

12. Any data subject who has suffered material or non-material damage as a result of an infringement of the GDPR *"shall have the right to receive compensation from the controller or processor for the damage suffered"* (Article 82(1)). Article 82(2) provide that *"Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation"*.

13. Article 82(6) of the GDPR provides that *"[c]ourt proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)."*

England

14. From 25 May 2018, the Data Protection Act 2018 ("2018 Act (UK)") provides a comprehensive legal framework for data protection in the United Kingdom. It sits alongside the GDPR, and, subject to the express provisions in the GDPR, adapts how the GDPR applies in the United Kingdom.

15. The domestic modifications are relatively minor, given that the GDPR is directly effective, and its implementation can only be adapted to the extent expressly provided for in the GDPR. By way of illustration, there are a number of exceptions set out under s.15 of the 2018 Act (UK),

read with Schedules 2, 3 and 5 to the 2018 Act (UK), which have been made pursuant to Articles 23, 85 and 89 of the GDPR. Section 10 of the 2018 Act (UK) also sets out additional conditions relating to the processing of special categories of personal data, which have been made pursuant to Article 9 of the GDPR.

16. As regards domestic enforcement, a data subject's right to complain, to an effective remedy and to compensation protected under the GDPR are all addressed in Part 6 of the 2018 Act (UK).

(1) Section 165(1) confirms that data subjects have a right to complain to the Information Commissioner's Office if the data subject considers that "*in connection with personal data relating to him or her, there is an infringement of the GDPR*". The Information Commission's Office ("ICO") is an independent body set up to protect and uphold information rights in the United Kingdom. If the complaint is not appropriately progressed, a court may compel the ICO to take appropriate steps: see s.166.

(2) Section 167 confers a power on "*data subjects*" to obtain a compliance order from a court. Section 167(1) provides that "*if, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation*". The court may make an order for "*the purposes of securing compliance with the data protection legislation*" (s.167(2)). Section 167(4)(a) provides that "*the reference to an application by a data subject includes an application made in exercise of the right under Article 79(1) of the GDPR (right to an effective remedy against a controller or processor)*".

(3) Section 168 confers a right on "*data subjects*" to compensation for breaches of the GDPR. Section 168(3) provides that "*[t]he court may make an order providing for the compensation to be paid on behalf of the person to: (a) the representative body, or (b) such other person as the court thinks fit*".

17. Although the UK ceased to be an EU Member State on 31 January 2020, the UK remains in a "*transition period*". Substantive EU law will continue to apply in the UK during the "*transition period*" between 31 January 2020 and 31 December 2020: Article 127(1) of the Withdrawal

Agreement, and s.1A(2) of the European Union (Withdrawal) Act 2018 (as amended by s.1 of the European Union (Withdrawal Agreement) Act 2020). The latter provides: "*The European Communities Act 1972, as it has effect in domestic law or the law of a relevant territory immediately before exit day, continues to have effect in domestic law or the law of the relevant territory on and after exit day so far as provided by subsections (3) to (5).*"

18. The "*transition period*", currently due to end on 31 December 2020, can be extended by one or two years if both the UK and the EU agree, provided that this is settled before 1 July 2020 (Article 132 of the Withdrawal Agreement).

19. At the end of the "*transition period*", the UK Government's stated position is to maintain the GDPR as retained EU law under the European Union (Withdrawal) Act 2018 and the necessary adjustments have been made under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (see §2.7 of the Explanatory Memorandum to those Regulations).

20. For completeness, I note that the 2018 Act (United Kingdom) is complemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("2003 Regulations"), which implements the European Directive 2002/58/EC ("the E-Privacy Directive"). The 2003 Regulations set out more specific privacy rights for particular electronic communications (including, amongst other things, unsolicited electronic communications made by phone, email and SMS). There is a right to bring civil proceedings for compensation for failure to comply with the 2003 Regulations: see regulation 30.

Ireland

21. From 25 May 2018, the key legislation in Ireland is the Data Protection Act 2018 ("2018 Act (Ireland)"). Similar to the position in the UK, the GDPR applies by default to personal data processing in Ireland, with limited modification set out in the 2018 Act (Ireland). Those modifications are primarily set out under Part 3 of the 2018 Act (Ireland).

22. A data subject's rights to an effective remedy and compensation under the GDPR are set out in Part 6 (of the 2018 Act (Ireland) ("*Enforcement of Data Protection Regulation and Directive*").

Under Irish law, a claimant has the right to relief by way of injunction or declaration, or compensation.

23. Section 117(1) provides that:

> *"[s]ubject to subsection (9), and without prejudice to any other remedy available to him or her, including his or her right to lodge a complaint, a data subject may, where he or she considers that his or her rights under a relevant enactment have been infringed as a result of the processing of his or her personal data in a manner that fails to comply with a relevant enactment, bring an action (in this section referred to as a "data protection action") against the controller or processor concerned."*

24. Section 117(2) provides that *"[a] data protection action shall be deemed, for the purposes of every enactment and rule of law, to be an action founded on tort."* Pursuant to s.117(3), *'[t]he Circuit Court shall, subject to subsections (5) and (6), concurrently with the High Court, have jurisdiction to hear and determine data protection actions"*.[10]

25. Section 117(4) provides that the court hearing a data protection action shall have the power to grant to the data subject one or more than one of the following forms of relief:

(1) relief by way of injunction or declaration; or

(2) compensation for damage suffered by the plaintiff as a result of the infringement of a relevant enactment.

26. Section 117(10) provides that '*damages*' includes material and non-material damage, and '*injunction*' means an interim injunction, interlocutory injunction, or an injunction of indefinite duration.[11]

---

[10] Sub-section (5) provides: *"The compensation recoverable in a data protection action in the Circuit Court shall not exceed the amount standing prescribed, for the time being by law, as the limit of that court's jurisdiction in tort"*. Sub-section (6) provides: *"The jurisdiction conferred on the Circuit Court by this section may be exercised by the judge of any circuit in which – (a) the controller or processor against whom the data protection action is taken has an establishment, or (b) the data subject has his or her habitual residence"*.

[11] This is in contrast to the pre-GDPR position under Irish law (discussed in further detail below), under which a plaintiff alleging loss arising from a data protection infringement needed to establish there had been a breach, that they had suffered damage, and that the breach had caused the damage (*i.e.* non-material loss was not recoverable). See *Collins v FBD Insurance plc* [2013] IEHC 137.

27. As in the United Kingdom, the GDPR regime is complemented by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI No. 336 of 2011), commonly referred to as the "*ePrivacy Regulations*", which implements the E-Privacy Directive.

(2) Data privacy protection prior to the implementation of GDPR

England

28. Prior to 25 May 2018 (i.e. prior to the GDPR and the 2018 Act (UK)), the processing of personal data in the United Kingdom was governed by the Data Protection Act 1998 ("1998 Act"), which implemented European Directive 95/46/EC ("the Data Protection Directive") into UK law.[12]

29. The 1998 Act required those handling personal data to comply with eight core data protection principles, and conferred data subjects with significant number of rights in relation to their personal information.

30. The key features of the 1998 Act can be summarised as follows:

(1) The 1998 Act applied to a "*data controller*" in respect of "*personal data*" where (i) the data controller was established in the UK and the personal data was processed in the context of that establishment; and (ii) the data controller was not established in the UK but used equipment located in the UK for processing the "*personal data*" otherwise than for the purposes of transit through the UK (s.5(1)).

(2) "*Personal data*" was defined as "*data which relates to a living individual who can be identified; (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual*" (s.1).

[12] In contrast to the GDPR, the Data Protection Directive did not have direct effect without domestic enactment because it was a Directive: Article 288 TFEU.

(3) "*Data controller*" was defined as "*a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed*" (s.1).

(4) The core of the 1998 Act are eight principles for handling personal data, which are set out in Schedule 1, Part 1. Any person that handled personal data was obliged to comply with the following principles (see s.4(4)). It will be apparent that there is considerable overlap between these principles, and the six principles set out under Article 5 of the GDPR.

(i) Principle 1: personal data must be processed fairly and lawfully.

(ii) Principle 2: personal data must be obtained only for specified and lawful purposes.

(iii) Principle 3: personal data must be adequate, relevant and not excessive.

(iv) Principle 4: personal data must be accurate and kept up to date.

(v) Principle 5: personal data must not be kept for longer than necessary.

(vi) Principle 6: personal data must be processed in accordance with the rights of data subjects.

(vii) Principle 7: there must be measures against unauthorised or unlawful processing of personal data.

(viii) Principle 8: there must be adequate protection for personal data transferred outside the EEA.

(5) "*Data subjects*" (i.e. individuals) are afforded a range of rights under the 1998 Act. These include:

(i) the right of access to personal data (s.7);

(ii) the right to prevent processing likely to cause damage or distress (s.10);

(iii) the right to prevent processing for purposes of direct marketing (s.11);

(iv) rights in relation to automated decision-taking (s.12); and

(v) the right to rectification, blocking, erasure and destruction (s.14).

31. In the United Kingdom, an independent authority has been established (the ICO) to protect and uphold privacy and information rights, including under the 1998 Act. Part V of the 1998 Act provides the methods by which the ICO can seek to ensure that data controllers comply with the provisions of the Act. It is relevant to note that Facebook was investigated by the ICO pursuant to the powers under the 1998 Act in respect of matters relating to Cambridge Analytica. The 19 June 2018 Notice of Intent published by the ICO stated that it considered that Facebook had processed personal data in breach of the first and seventh data protection principles set out in Schedule 1 to the 1998 Act, and thereby breached s.4(4) of the 1998 Act (§8). On 30 October 2019 it was announced that this process was closed following a settlement between Facebook and the ICO.

32. In addition to the powers of enforcement given to the ICO, an individual who is the subject of loss or distress may bring court proceedings against the data controller for compensation. In this regard, Article 22 of the Data Protection Directive provided that:

> *"Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question."*

33. Article 23 of the Data Protection Directive further provided that:

> "(1) *Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.*
>
> *(2) The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage."*

34. This was reflected in s.13(1) of the 1998 Act, which provided:

> *"[a]n individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage."*

35. Section 13(2) of the 1998 Act provided that *"an individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if – (a) the individual also suffers damage by reason of the contravention, or the contravention relates to the processing of personal data for the special purposes."*[13] In proceedings brought against a person by virtue of s.13, it was *"a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned"* (s.13(3)).

36. Pursuant to s.14(4), if a court is satisfied on the application of a data subject:

(1) that he has suffered damage by reason of any contravention by a data controller of any of the requirements of the 1998 Act in respect of any personal data, in circumstances entitling him to compensation under s.13, and

(2) that there is a substantial risk of further contravention in respect of those data in such circumstances,

the court could order the rectification, blocking, erasure or destruction of any of those data.

37. There has been debate in the English courts regarding the nature of the damage that an individual needed to have suffered before triggering an entitlement to compensation (i.e. whether an individual must suffer pecuniary loss). The current position is set out in *Lloyd v Google LLC* [2020] 2 WLR 484, where the Court of Appeal followed the decision in *Gulati v MGN Ltd* [2017] QB 149 in holding that a claimant could recover damages for loss of control of their data under the 1998 Act *without* proving either pecuniary loss or distress. I understand that permission to appeal has been granted for the case to be heard by the Supreme Court.

[13] The scope of s.13(2) was interpreted in *Lloyd v Google LLC* [2020] 2 WLR 484, discussed below.

38. For examples of award for non-pecuniary loss in claims for infringement, see, e.g., *Halliday v Creation Consumer Finance Ltd* [2013] 3 CMLR 4 (£750); *AB v Ministry of Justice* [2014] EWHC 1847 (QB) (£2,250); and *TLT v Home Office* [2016] EWHC 2217 (QB) (£12,500, £12,500, £6,000, £3,000, £3,000, and £2,500).

39. The transitional provisions for the 1998 Act are set out in Schedule 20 to the 2018 Act (UK). Paragraph 6 of Schedule 20 relevantly provides: "*The repeal of section 13 of the 1998 Act (compensation for failure to comply with certain requirements) does not affect the application of that section after the relevant time in relation to damage or distress suffered at any time by reason of an act or omission before the relevant time.*"

Ireland

40. Prior to 25 May 2018 (i.e. prior to the GDPR and the 2018 Act (Ireland)), the processing of personal data in Ireland was governed by the Data Protection Act 1988 ("1988 Act") (as amended by the Data Protection (Amendment) Act 2003 ("2003 Act")), which implemented the Data Protection Directive into Irish law. The 1988 Act and the 2003 Act continue to apply to ongoing investigations by, and complaints to, the Data Protection Commissioner commenced or made before 25 May 2018, and new complaints and potential contraventions of the 1988 Act or 2003 Act which arose prior to the 25 May 2018, but which are made or investigated on or after 25 May 2018: see 2018 Act (Ireland) ss.7(4) and 8.

41. Section 2(1) of the 1988 Act provides:

> "*A data controller shall, as respects personal data kept by him or her, comply with the following provisions:*
>
> *(a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,*
>
> *(b) the data shall be accurate and complete and, where necessary, kept up to date,*
>
> *(c) the data –*
>
> *(i) shall have been obtained only for one or more specified, explicit and legitimate purposes,*

(ii) *shall not be further processed in a manner incompatible with that purpose or those purposes,*

(iii) *shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and*

(iv) *shall not be kept for longer than is necessary for that purpose or those purposes,*

(d) *appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing".*

42. "*Data subjects*" (i.e. individuals) are afforded a range of rights under the 1988 Act. These include:

(1) the right to be informed of the existence of processing of one's personal data (s.3);

(2) the right of access (s.4);

(3) the right to rectify, block or erase any data (s.6);

(4) the right to object to processing likely to cause damage or distress (s.6A); and

(5) the right not to be subject to automated decisions (s.6B).

43. As in the UK, Article 22 and 23 of the Data Protection Directive are reflected in the 1988 Act. Section 7 provides:

> *"For the purposes of the law of torts and to the extent that the law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned".*

44. This imposes a duty of care upon data controllers, who must take reasonable care not to breach that duty: see, generally, D. Kelleher, *Privacy and Data Protection in Ireland* (2nd edition, 2015), pp.399-404. In contrast to the position under English law, the Irish case-law suggests that a plaintiff can only recover compensation for breach of data protection law if he or she can show

actual loss or actual damage caused by that breach: see *Collins v FBD Insurance* [2013] IEHC 137.

(3) Breach of confidence

England

45. Breach of confidence is an equitable doctrine that allows an individual to claim a remedy when their confidence has been breached.[14] As the House of Lords observed in *Campbell v MGN* [2004] 2 AC 457, "*[t]he common law or, more precisely, courts of equity have long afforded protection to the wrongful use of private information by means of the cause of action which became known as breach of confidence*" (§13).

46. A summary of the doctrine can be found in the judgment of Lord Neuberger in *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] 1 WLR 1556:

> "22. *[A]n action in breach of confidence is based ultimately on conscience. As Megarry J said in Coco v A N Clark (Engineers) Ltd [1969] RPC 41, 46, 'the equitable jurisdiction in cases of breach of confidence is ancient; confidence is the cousin of trust.'*
>
> 23. *The classic case of breach of confidence involves the claimant's confidential information, such as a trade secret, being used inconsistently with its confidential nature by a defendant, who received it in circumstances where she had agreed, or ought to have appreciated, that it was confidential: see eg per Lord Goff of Chieveley in Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109 , 281. Thus, in order for the conscience of the recipient to be affected, she must have agreed, or must know, that the information is confidential.*
>
> ...
>
> 25. *Liability for breach of confidence is not, of course, limited to such classic cases. Thus, depending on the other facts of the case, a defendant who learns of a trade secret in circumstances where she reasonably does not appreciate that it is confidential, may none the less be liable to respect its confidentiality from the moment she is told, or otherwise appreciates, that it is in fact confidential. From that moment, it can be said that her conscience is affected in a way which should be recognised by equity.*"

[14] Equity is the body of law which was developed in the English Court of Chancery to sit alongside the common law.

47. More recently, in *Kerry Ingredients (UK) Ltd v Bakkavor Group Ltd* [2016] EWHC 2448 (Ch), Newey J confirmed that the '*core test*' is to be found in Arnold J's judgment in *Force India Formula One v Malaysia Racing Team* [2012] EWHC 616 (Ch) ('Force India Formula One'), in which the Court held (at §224):

> *"[a]n equitable obligation of confidence will arise as a result of the acquisition or receipt of confidential information if, but only if, the acquirer or recipient either knows or has notice (objectively assessed by reference to a reasonable person standing in his shoes) that the information is confidential."*

48. As to unauthorised use, *"[t]he fact that a defendant has not precisely replicated the relevant confidential information need not mean that he did not use it.'*[15] In *Force India Formula One*, the High Court confirmed that *"[o]nce an equitable obligation of confidence has arisen .... the person subject to the obligation may be held liable for acting in breach of it even though he is not conscious of doing so"*.[16]

49. A claimant may bring an action based on an actual or threatened breach of confidence. As a general rule, an action for breach of confidence may be brought only by a person to whom the duty in question is owed. However, an action for protective relief may be exceptionally brought by someone having responsibility to protect the welfare of that person.[17]

50. The remedies that a claimant seeks will depend on whether the confidential information has already been disseminated. In general, a successful action for breach of confidence could result in one or more of the following remedies: an injunction, an account of profits, compensation (damages), delivery up or destruction of documentation containing the relevant information, or declaration. If the confidential information has not yet been disseminated, or if there is a risk of further dissemination, the claimant may seek to obtain an injunction to restrain the dissemination of the information in question.

51. Insofar as a claim for breach of confidence engages equitable principles, the usual barriers to equitable relief may apply (*e.g.* damages are an equitable remedy entirely at the discretion of

---

[15] *Kerry Ingredients (UK) Ltd v Bakkavor Group Ltd* [2016] EWHC 2448 (Ch), §72.
[16] *Force India Formula One Team v Malaysia Racing Team* [2012] EWHC 616, §240.
[17] *Fraser v Evans* [1969] 1 QB 349.

the court; the court has a discretion to refuse or limit equitable relief in cases where the claimant is not seen to come with '*clean hands*' and/or has not acted with reasonable promptness in bringing the claim).

Ireland

52. The equitable doctrine of breach of confidence is also recognised under Irish law. In *Mahon v Post Publications Ltd* [2007] 3 IESC 338, the Supreme Court confirmed that the requirements for a successful action based on a breach of an equitable duty of confidence are as stated by Megarry J in *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41 (see §46 above). In *Mahon v Post Publications Ltd*, Fennelly J summarised the key elements of the doctrine in the following terms (at §74):

> *"1. The information must in fact be confidential or secret: it must ... "have the necessary quality of confidence about it".*
>
> *2. It must have been communicated by the possessor of the information in circumstances which impose an obligation of confidence or trust on the person receiving it.*
>
> *3. It must be wrongfully communicated by the person receiving it or by another person who is aware of the obligation of confidence."*

53. The principles set out above were recently affirmed in *McCann & Ors v The Trustees of the Victory Christian Fellowship* [2015] IECA 117.

54. A plaintiff in Ireland may pursue an action based on a breach of the equitable duty of confidence. As is the case in England, the remedies that a plaintiff seeks will depend on whether the confidential information has already been disseminated, and may be restricted or limited by the usual barriers to equitable relief.

55. In relation to damages, in *Slattery v Friends First Life Assurance Company Ltd* [2013] IEHC 136, the High Court observed (at §111):

> *"it is clear that the law recognises a duty of confidentiality such as would apply in this case, whether framed in contract, in tort, in equity, or on a constitutional basis, and that this Court is possessed of the jurisdiction to award damages on foot of a breach thereof."*

56. The High Court also confirmed that "*that the Court is vested with a discretion to award compensatory damages, including aggravated damages, notwithstanding any failure to explicitly plead the latter category*" (§121). In that case, the High Court awarded the plaintiff damages, including aggravated damages, for breach of confidentiality. With regard to aggravated damages, the Court observed that (§123):

> "*[t]he breach of confidence was a serious one and was deliberately intended to cause harm to the plaintiff's business interests … It was a quite improper use of information gathered in the course of a fiduciary relationship. The plaintiff is entitled to be compensated for the deliberate and conscious breach of his right to confidentiality, involving an extraordinary, wilful and totally inappropriate dissemination of this information…*".

(4) Misuse of private information

57. In recent years the action for breach of confidence has developed in the English courts to protect privacy interests, into a distinct, but related, tort for the misuse of private information. This has, in part, been influenced by the incorporation of the ECHR into domestic law by the Human Rights Act 1998 (see further §69 below). It has for some years been widely accepted that "*there are now two separate and distinct causes of action: an action for breach of confidence; and one for misuse of private information*": *Vidal-Hall v Google Inc* [2016] QB 1003, §21. See also *Axon v Ministry of Defence* [2016] EWHC 787 (QB), §35 (noting that the tort of misuse of private information is now "*clearly recognised as an actionable wrong*").

58. An action for misuse of private information requires consideration of two issues:

(1) First, whether the information is private, in the sense that it is protected by Article 8 ECHR. The European Court of Human Rights and domestic courts have had no difficulty in finding that the gathering, storing and release of information relating to an individual's private life falls within the scope of Article 8 ECHR: for a recent analysis see *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 672.

(2) Secondly, if there is a "*reasonable expectation of privacy*," the court will need to consider whether there has been an infringement of the right to privacy. This requires weighing up the reasonable expectation of privacy against any countervailing rights of the defendant, and any third parties.

59. A claimant can bring a civil action in tort for the misuse of information. Within this, a claimant may seek an injunction (e.g., to prevent publication of the private information) and/or damages to compensate for the loss (including, for example, distress) caused by the misuse of their information. As *Toulson and Phipps on Confidentiality* (2020) observes:

> *"[t]he majority of reported cases relating to the alleged misuse of private information involve applications for restraining injunctive relief, on either an interim or a final basis. As a general rule, injunctions are not granted when damages constitute an adequate remedy, but it is in the nature of privacy claims that this will rarely be the case."*[18]

60. Alongside injunctions, compensation by way of general damages is '*the other principal remedy usually provided for misuse of private information.*'[19] In relation to the quantum of damages in this context, the Court observed in *Mosley v News Group Newspapers* [2008] EMLR 20 (at §231):

> *"[A]n infringement of privacy cannot ever be effectively compensated by a monetary award. Judges cannot achieve what is, in the nature of things, impossible. That unpalatable fact cannot be mitigated by simply adding a few noughts to the number first thought of. Accordingly, it seems to me that the only realistic course is to select a figure which marks the fact that an unlawful intrusion has taken place while affording some degree of solatium to the injured party. That is all that can be done in circumstances where the traditional object of restitution is not available. At the same time, the figure selected should not be such that it could be interpreted as minimising the scale of the wrong done or the damage it has caused."*

61. The leading authority on the quantum of damages for misuse of private information is *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch), in which Mann J awarded not only damages for distress, but also an element for the loss of privacy or autonomy (§168).[20] On appeal, Arden LJ confirmed that "*[t]he essential principle is that, by misusing their private information, MGN deprived the claimants of their right to control the use of private information*".[21]

62. The Court of Appeal has held that there is no requirement that an individual have suffered any pecuniary loss in order to trigger an entitlement to damages. Thus, in *Vidal-Hall v Google* [2016] QB 1003, the Court held that individual users who claimed that their data was collected

---

[18] Charles Phipps, William Harman and Simon Teasdale (eds), *Toulson and Phipps on Confidentiality* (2020), §7-186.

[19] Charles Phipps, William Harman and Simon Teasdale (eds), *Toulson and Phipps on Confidentiality* (2020), §7-187.

[20] *Gulati and Ors v MGN Ltd (un-redacted)* [2015] EWHC 1482 (Ch), §168.

[21] *Representative Claimants v MGN Ltd* [2017] QB 149, §45.

by Google without their consent for the purposes of more effectively targeting advertising were entitled to seek damages, despite the lack of pecuniary loss.

(5) Constitutional right to privacy

63. Bunreacht na hÉireann ("the Constitution") does not explicitly guarantee a right to privacy, but the courts have recognised an unenumerated right to privacy as one of the personal rights in the Constitution protected under Article 40.3.1, which provides "*[t]he State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of citizens*".

64. The constitutional right to privacy was first recognised in the case of *McGee v Attorney General* [1974] IR 284. In *Kennedy v Ireland* [1987] 1 IR 587, the High Court expressly recognised that (at 592),

> "*[t]hough not specifically guaranteed by the Constitution, the right of privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State.*"[22]

65. This right is not unqualified and may be restricted by the constitutional rights of others, by the requirements of the common good and is subject to the requirements of public order and morality (*id*).

66. In *Herrity v Associated Newspapers [Ireland] Ltd* [2008] IEHC 249, Dunne J reviewed the Irish caselaw beginning with *McGee*, and provided the following summary:

> "*(1) There is a Constitutional right to privacy.*
>
> *(2) The right to privacy is not an unqualified right.*
>
> *(3) The right to privacy may have to be balanced against other competing rights or interests.*

[22] *Kennedy v Ireland* [1987] 1 IR 587, 592.

(4) *The right to privacy may be derived from the nature of the information at issue – that is, matters which are entirely private to an individual and which it may be validly contended that there is no proper basis for the disclosure either to third parties or to the public generally.*

(5) *There may be circumstances in which an individual may not be able to maintain that the information concerned must always be kept private, having regard to the competing interests which may be involved but may make complaint in relation to the manner in which the information was obtained."*

67. The constitutional right of privacy includes a right to a remedy. Hence, a person who apprehends an interference with her privacy rights may seek injunctive relief to prevent such interference, and a person who suffers damage as a consequence of such an interference may seek to recover damages. Importantly, "*[t]he right to sue for damages for breach of the constitutional right to privacy is not confined to actions against the State or State bodies or institutions*"; in addition, it "*is actionable against a private person or entity*".[23]

(6) Article 8 ECHR

68. The right to respect for private and family life, as protected under Article 8 of the EHCR, has been incorporated into UK domestic law through the Human Rights Act 1998. Schedule 1 Part 1 of the HRA sets out each of the ECHR rights and freedoms, including Article 8. Section 6(1) of the Human Rights Act 1998. provides that "*[i]t is unlawful for a public authority to act in a way which is incompatible with a Convention right'. 'Public authority'* is defined by subsection (3) to include: '*(a) a court or tribunal, and (b) any person certain of whose functions are functions of a public nature*". Thus, a public authority must not act in any way that is incompatible with an individual's Article 8 rights.

69. The Human Rights Act 1998 also provides a mechanism by which an individual can bring a claim for a breach of Article 8 (see s.7(1)), however a claim can only be brought against a public authority. Article 8 of the ECHR is not directly effective against private litigants, and s.7 of the Human Rights Act 1998 does not provide a standalone private cause of action for a breach of Article 8. However, as explained above, Article 8 is relevant to, and has had an influence on

[23] *Herrity v Associated Newspapers [Ireland] Ltd* [2008] IEHC 249.

private causes of action, including, in particular, breach of confidence and the tort of misuse of public information.

70. The same applies in Ireland: see European Convention on Human Rights Act 2003, which similarly provides a mechanism by which an individual can bring a claim against the State for a breach of Article 8: see s.3. The provision does not provide a standalone private cause of action for breach of Article 8 (*contra* the position in relation to breaches of the constitutional right, which may be awarded against private citizens, and not just the State).

C. JURISDICTION AND CHOICE OF LAW CLAUSE

71. If the UK plaintiffs were excluded from the class in the MDL, they would be free to commence individual civil claims based on any of the rights set out above. As noted above, I am instructed that the UK plaintiffs' contractual counterparty and the data controller in respect of their data on the Facebook platform was at all material times Facebook Ireland Limited ("Facebook Ireland"). Any claim for breach of the Terms of Service or the duties of a data controller under the data protection legislation would be against Facebook Ireland, not Facebook, Inc.

72. For the reasons set out below, to the extent that the UK plaintiffs are consumers they would be able to commence their individual claims in the courts of England and Wales (or Scotland if applicable) or Ireland. To the extent that the UK plaintiffs are not consumers, they would be required to commence any claim in the courts of Ireland. In either case, the applicable law will depend on a number of factors but it is likely that the UK plaintiffs will be able to rely on English or Irish law.

73. Those claims would be likely to be governed by clause 4 of the "Terms of Service" applicable to Facebook's UK users. This provides as follows:

> *"If you are a consumer and habitually reside in a Member State of the European Union, the laws of that Member State will apply to any claim, cause of action or dispute that you have against us, which arises out of or relates to these Terms or the Facebook Products ("claim"), and you may resolve your claim in any competent court in that Member State that has jurisdiction over the claim. In all other cases, you agree that the claim must be resolved in a competent court in the Republic of Ireland and that Irish law will govern these Terms and any claim, without regard to conflict of law provisions".*

74. These "Terms of Service" replaced the "Statement of Rights and Responsibilities" (the January 2015 version of which I have reviewed).

75. Clause 15.1 of the Statement of Rights and Responsibilities contained an exclusive jurisdiction clause in favour of "*the U.S. District Court for the Northern District of California or a state court located in San Mateo County*". Clause 18.1 of the Statement of Rights and Responsibilities provided that "[i]*f you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited…*"

76. I understand that clause 4 of the Terms of Service was an amendment to the contract between Facebook Ireland and UK users. I understand that the UK users who continued to use Facebook services after the introduction of the Terms of Service consented to that amendment. Accordingly, clause 4 of the Terms of Service replaced clause 15.1 of the Statement of Rights and Responsibilities.

77. The interpretation of the scope of a jurisdiction clause falls to be considered at the time that jurisdiction agreement is made and the question as to whether a claim falls within the jurisdiction clause is an issue that has to be determined at the time the proceedings are issued: *BNP Paribas v Trattamento Rifuti Metropolitani SpA* [2019] EWCA Civ 768 §§56, 60. In my view, an Irish court would take the same view. Since clause 4 of the Terms of Service was agreed to cover all disputes after 2018 and since it was obvious that such disputes could arise from events which preceded 2018 (as well as events after 2018), an English or an Irish court is very likely to construe clause 4 as covering any claim sought to be issued by a UK plaintiff.

78. A contrary interpretation would make no sense in my view. It is inherently unlikely that parties to a contract would choose to have future claims determined in different countries and under different legal systems depending simply on the date upon which the alleged wrongdoing occurred. Such a result would require clear language. As a matter of language, the parties have clearly decided to have all disputes after the change in terms determined according to the new dispute resolution provision in clause 4 regardless of when the underlying alleged wrongdoing occurred.

79. As regards the scope of clause 4, in my view it is sufficiently broad to catch not only any breaches of the contract between Facebook Ireland and the user but also the non-contractual claims set out above. That arises from (i) the language of clause 4 (covering not merely disputes relating to "these Terms" but also, and separately, "the Facebook Products" themselves); and (ii) the fact that the non-contractual claims would be closely linked to the kinds of complaints which could be made about a breach of the Terms. The complaints appear to allege breaches of principles to which Facebook was alleged to have committed contractually: *Fiona Trust v Privalov* [2007] 4 All ER 951 at §13, *Microsoft Mobile Oy v Sony Europe Ltd* [2017] EWHC 374 §72, *Ryanair Ltd v Esso Italiana Srl* [2015] 1 All ER (Comm) §53.

80. Clause 4 consists of (1) a non-exclusive jurisdiction and choice of law agreement in favour of a Facebook consumer user's own court and national law where he resides in a Member State of the EU; and (2) an exclusive jurisdiction and choice of law agreement in favour of the courts of Ireland and Irish law in all other cases.[24]

81. To the extent that the UK plaintiffs are not "consumers" within the meaning of EU law (as implemented in UK and Irish law) and post-Brexit UK law:

(1) The exclusive jurisdiction agreement in clause 4 would apply to such claims and it is likely that the choice of law agreement in clause 4 would apply also. The claims would be required to be issued in the courts of Ireland and they would likely be subject to Irish law.

(2) In Irish law (and in English law up until 31 December 2020), the jurisdiction agreement would be binding under Article 25 of the Brussels Recast Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ("the Brussels Recast Regulation"). In English law from 1 January 2020, it would bind as a matter of contract law.

[24] The UK ceased to be a Member State of the EU on 31 January 2020. After that date, the UK plaintiffs ceased to be habitually resident in a Member State of the EU. Accordingly, the non-exclusive jurisdiction and choice of law clause in clause 4 would not apply to a claim issued by such a person after 31 January 2020.

(3) As regards choice of law, the parties' own choice will apply to any contractual claims.[25] As regards non-contractual claims, the applicable law will depend on a number of factors but Irish law is likely to apply.[26]

82. To the extent that the UK plaintiffs are consumers pursuing their individual claims, the position is as follows.

83. Until 31 December 2020, the issue of jurisdiction in respect of claims issued by the UK plaintiffs would be governed by the Brussels Recast Regulation. The Brussels Recast Regulation continues to apply in UK law[27] until the end of the current transition period pursuant to the European Union (Withdrawal Agreement) Act 2020 and Articles 66-69 of the Withdrawal Agreement between the UK and the EU.

84. Section 4 of the Brussels Recast Regulation contains Articles 17-19 and deals with "[j]*urisdiction over consumer contracts*". Article 18 of the Brussels Recast Regulation provides that:

> "*A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled*".

85. Article 19 of Brussels Recast Regulation provides that:

> "*The provisions of this Section may be departed from only by an agreement: (1) which is entered into after the dispute has arisen; (2) which allows the consumer to bring proceedings in courts other than those indicated in this Section; or (3) which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which confers jurisdiction on the courts*

---

[25] Regulation 593/2008 on the law applicable to contractual obligations ("Rome I"), Article 3(1).

[26] To the extent that Regulation 864/2007 on the law applicable to non-contractual obligations ("Rome II") applies (and both Rome I and II are retained EU law in the UK under The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019), the parties' choice will bind them (Article 14); to the extent that Rome II is inapplicable (*per* Article 1(2)(g)), in England the Private Law (Miscellaneous Provisions) Act 1995 will likely govern the question (ss. 11-12) and Dicey, Morris & Collins, *The Conflicts of Laws* (15th ed.) §34-091-092, and in Ireland, the common law (*An Bord Trachtala v Waterford Foods* [1994] FSR 516).

[27] I use "UK law" as a shorthand for the common provisions of the laws of England and Wales, the laws of Scotland and Northern Ireland.

of that Member State, provided that such an agreement is not contrary to the law of that Member State".

86. After 31 December 2020 (when the Brussels Recast Regulation will cease to apply in the UK), s. 15B[28] of the Civil Jurisdiction and Judgments Act 1982 will come into force. This provision (which effectively continues the protection under Articles 18-19 of the Brussels Recast Regulation) provides as follows:

> *"(1) This section applies in relation to proceedings whose subject-matter is a matter relating to a consumer contract where the consumer is domiciled in the United Kingdom.*
>
> *(2) The consumer may bring proceedings against the other party to the consumer contract –*
>
> *(a) where the other party to the consumer contract is domiciled in the United Kingdom, in the courts of the part of the United Kingdom in which the other party to the consumer contract is domiciled, or*
>
> *(b) in the courts for the place where the consumer is domiciled (regardless of the domicile of the other party to the consumer contract).*
>
> ...
>
> *(6) Subsections (2)... may be departed from only by an agreement –*
>
> *(a) which is entered into after the dispute has arisen,*
>
> *(b) which allows the consumer to bring proceedings in courts other than those indicated in this section, or*
>
> *(c) which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the United Kingdom and in the same part of the United Kingdom, and which confers jurisdiction on the courts of that part of the United Kingdom, provided that such an agreement is not contrary to the law of that part of the United Kingdom.*
>
> *(7) For the purposes of this section, where a consumer enters into a consumer contract with a party who is not domiciled in the United Kingdom, the other party to the contract is deemed to be domiciled in a particular part of the United Kingdom if that party has a branch, agency or*

[28] Inserted by amendment under reg. 26 of the Civil Jurisdiction and Judgments (Amendment) (EU Exit) Regulations 2019 (SI 2019/479).

establishment in that part of the United Kingdom and the dispute arose out of the operations of that branch, agency or establishment".

87. Thus, before and after 31 December 2020, the UK consumer plaintiffs will be able to issue their individual claims in the courts of England and Wales (or Scotland if applicable) or the Irish courts. As regards the applicable law, that will be English law in respect of any contractual claims pursuant to the terms of Rome I (Article 6(1). As regards non-contractual claims, the applicable law will depend on a number of factors but is likely to be Irish law or English law.[29]

88. Any judgment obtained in favour of a UK plaintiff in an English court may be enforced in an Irish court under the Irish common law rules.[30] It is unlikely that the Hague Convention on Choice of Court Agreements 2005 (to which both Ireland and the UK are parties) will apply to such enforcement. First, consumer claims are excluded: Article 2(1). Secondly, it is a condition of enforcement under the Hague Convention that the judgment is made by a court chosen by the parties pursuant to an exclusive jurisdiction agreement: Article 8(1). That would not be the English court, in the circumstances described above.

D. RES JUDICATA AND ABUSE OF PROCESS

(1) The position if a claimant does not fall within the Proposed Class in the MDL

England

89. The doctrine of *res judicata* operates such that once "*the res – the thing actually or directly in dispute – has been already adjudicated upon, … by a competent court, it cannot be litigated again.*"[31] The longstanding policy underpinning *res judicata* is that there is a public interest in the finality of litigation.

90. The general doctrine comprises two distinct rules: *cause of action estoppel* and *issue estoppel*.

[29] The legislation is listed in footnote 25.
[30] *Re Flightlease* [2012] IESC 12.
[31] *Ord v Ord* [1923] 2 KB 432, 439.

(1) *Cause of action estoppel* arises where the cause of action in the latter proceedings is identical to that determined in earlier proceedings. As Lord Sumption explained in *Virgin Atlantic Airways Ltd v Zodiac Seats UK Ltd* [2014] AC 160, *"once a cause of action has been held to exist or not to exist, that outcome may not be challenged by either party in subsequent proceedings"* (§17).

(2) *Issue estoppel* arises where a particular issue formed a necessary ingredient in a cause of action that has been litigated and decided and, in subsequent proceedings between the same parties, involving a different cause of action in which the same issue is relevant, one of the parties seeks to reopen the issue: *Arnold v Natwest Bank* [1992] 2 AC 93, 105; *Mills v Cooper* [1967] 2 QB 459, 468.

91. Cause of action estoppel does not arise in the present context, given that the causes of action in any US and UK proceedings will not be the same.

92. The question as to whether an *issue estoppel* can be created by a foreign judgment was considered in *DSV Silo- und Verwaltungsgesellschaft mbH v Owners of the Sennar* [1985] 1 WLR 490. Lord Diplock set out the following conditions (at 493H):

> *"To make available an issue estoppel to a defendant to an action brought against him in an English court on a cause of action to which the plaintiff alleges a particular set of facts give rise, the defendant must be able to show (1) that the same set of facts has previously been relied on as constituting a cause of action in proceedings brought by that plaintiff against that defendant in a foreign court of competent jurisdiction and (2) that a final judgment has been given by that foreign court in those proceedings."*

93. Lord Brandon set out similar conditions (at 499B):

> *"in order to create an estoppel of that kind, three requirements have to be satisfied. The first requirement is that the judgment in the earlier action relied on as creating an estoppel must be (a) of a court of competent jurisdiction, (b) final and conclusive and (c) on the merits. The second requirement is that the parties (or privies) in the earlier action relied on as creating an estoppel, and those in the later action in which that estoppel is raised as a bar, must be the same. The third requirement is that the issue in the later action, in which the estoppel is raised as a bar, must be the same issue as that decided by the judgment in the earlier action."*

94. In a scenario where UK Facebook users are not part of the Proposed Class, then the position in law is straightforward. The principle of *res judicata* would not apply as the parties to the proceedings would not be the same: the claimants would *not* be the same, and it is also likely that the defendants would not be the same, given that, for the reasons discussed at §§4(2) and 71 above, it is very likely that Facebook Ireland would be a defendant in any English or Irish proceedings (and they are not a party in the MDL). The UK Facebook users would therefore be free to bring any data protection and/or privacy-based claim in the English or Irish courts.

95. In addition to the doctrine of *res judicata*, the abuse of process doctrine has also developed to protect the public interest in the finality of litigation. It typically arises in two scenarios:

(1) where a party seeks to raise a cause of action or an issue which, although not raised in earlier proceedings between the same parties, could have been raised in those proceedings (often described as the rule in *Henderson v Henderson* (1843) 3 Hare 100); or

(2) where a party seeks to mount a collateral attack upon a final decision which has been made against that party, in which that party had a full opportunity of contesting that decision in the court by which it was made.

96. A party may raise an abuse of process argument based on a foreign judgment, however it is only likely to succeed in very limited circumstances. As Professor Adrian Zuckerman explains:

> *"A party who bases an abuse of process argument on a foreign judgment must, in addition to the normal matters, satisfy the court that a person, who has a right of access to justice in this country, should be prevented from exercising it because he should have raised the matter abroad. A party will not be prevented from raising an issue in England, despite the fact that he could have raised it in foreign proceedings, if he had good reasons for not pursuing the issue abroad…*
>
> *The approach to collateral attacks on foreign judgments is more relaxed than in relation to domestic judgments because the public interest in avoiding conflicts with foreign decisions is not as strong as that of avoiding conflicts between domestic decisions."*[32]

97. The issue was considered at some length in *House of Spring Gardens Ltd and Ors v Waite and others* [1990] 1 QB 241. In that case, the Court held that even if the foreign judgment did not

[32] Zuckerman, *Principles of Civil Procedure* (3rd edition, 2013), §25.145.

create an estoppel (which it did on the facts), it was an abuse of the process of the court and contrary to justice and public policy for the issue of fraud to be re-litigated in the English court after the issue had been tried and decided by the Irish court. On the facts of that case, LJ Stuart-Smith stated:

> *"The question is whether it would be in the interests of justice and public policy to allow the issue of fraud to be litigated again in this court, it having been tried and determined by Egan J. in Ireland. In my judgment it would not; indeed, I think it would be a travesty of justice. Not only would the plaintiffs be required to re-litigate matters which have twice been extensively investigated and decided in their favour in the natural forum, but it would run the risk of inconsistent verdicts being reached, not only as between the English and Irish courts, but as between the defendants themselves.... Public policy requires that there should be an end of litigation and that a litigant should not be vexed more than once in the same cause."*[33]

98. In a scenario where UK Facebook users are not part of the Proposed Class, then the position in law on abuse of process is also straightforward. The *Henderson v Henderson* rule will clearly not be engaged. It is also highly unlikely that a Court would treat a claim as a collateral attack on the judgment in the MDL in circumstances where the UK Facebook users were not a party to those proceedings.

Ireland

99. The position in Ireland is similar to that in England: see, e.g., *Dominic Carney v Bank of Scotland Plc (formerly Bank of Scotland (Ireland) Limited) and Gearoid Costelloe)* [2017] IECA 295. The analysis set out above therefore applies.

(2) The position if a claimant does fall within the Proposed Class in the MDL

England

100. The position in law where a claimant does fall within the Proposed Class is less straightforward. If a UK claimant was an active participant in the MDL, or took compensation as part of the MDL, and the defendant/s were the same (which, for the reasons set out at §94 above,

[33] *House of Spring Gardens Ltd and Ors v Waite and others* [1990] 1 QB 241, 255B-D.

appears unlikely), it is possible that an English court would treat a future claim by that individual as blocked by issue estoppel and/or an abuse of process.

101. The position is more complicated in the context of opt-out proceedings, where, for instance, a UK claimant does not opt-out, but was entirely uninvolved in the US proceedings, and did not take any compensation. If, for instance, the claims against Facebook in the MDL were to fail, it may be quite likely that such a claimant would attempt to bring similar claims against Facebook in their home jurisdiction.

102. In such a scenario, the question arises as to whether such a claim would be precluded by the doctrine of *res judicata*, and/or constitute an abuse of process. I am not aware of any case-law that directly addresses this point. In my view, however, an English court is likely to find that such a claim would not be blocked by *res judicata* or an abuse of process for at least the four following reasons.

103. First, for the purposes of *res judicata*, in order for a foreign judgment to be treated as having a preclusive effect, the parties must be identical to the parties in the English action. The question as to whether an individual who has not participated in the US proceedings, but has not opted out of them, is a party, will be a matter for *English law* to decide. In this context, it is relevant to note that in the context of English representative proceedings, a represented person "*is not a party to the claim*" (see, e.g., CPR 19.6(4)(b) (although it may, ultimately, be binding on them).[34] Although there is scope for debate, in my view it is likely that an English Court would not treat a US judgment as *res judicata* in relation to a UK plaintiff in the US proceedings who failed to opt-out but did not take any compensation.[35]

[34] More generally, it is relevant to note that the Civil Procedure Rules in England do not recognise opt-out class actions. Pursuant to Part 19 of the Civil Procedure Rules, there is a process for group litigation (Group Litigation Orders or "GLOs"), however that requires parties to consent to involvement in the proceedings. The only area where opt-out proceedings are allowed, are in the Competition Appeal Tribunal for certain competition proceedings. In that context, specific legislation was enacted in order to allow for this.

[35] Support for this view can be found in academic commentary: see, e.g., R. Mulheron, "*The Recognition, and Res Judicata Effect, of a United States Class Actions Judgment in England: A Rebuttal of Vivendi*", *Modern Law Review*, 75(2) (2012) 180.

104. Secondly, as explained above, it is also likely that the defendant/s will not be the same, given it is very likely that Facebook Ireland would be a defendant in any English or Irish proceedings (and they are not a party in the MDL).

105. Thirdly, in order for *res judicata* and/or abuse of process to apply, it will be necessary to demonstrate that the issues in dispute are materially the same. In other words, were the particular issues that formed a necessary ingredient in the claims in the MDL the same issues that would be before a subsequent court in English proceedings. This is also likely to give rise to difficulties, particularly in the context of the data protection legislation that is in place in England and Ireland, which are materially different in scope and effect than any of the causes of action pursued in the MDL.

106. Fourthly, in the context of abuse of process, a court will take a broad, merits-based judgment which takes into account all of the public and private interests involved. The Court is less likely to be concerned about a collateral attack on a foreign judgment, based on entirely different claims (*cf House of Spring Gardens Ltd and Ors v Waite and others* [1990] 1 QB 241, where the causes of action were materially similar). In my view, a Court is unlikely to consider that a party is misusing or abusing the process of the Court by seeking to raise before it an issue which was addressed in the MDL, in circumstances where that party had no involvement at all in the MDL and, potentially, was not even aware of it. This will all ultimately turn on the individual facts and circumstances of the case.

Ireland

107. As noted above, the legal position is similar in Ireland, and, in my view, the analysis set out above is therefore likely to also apply under Irish law.

E. EVIDENCE AND THE HAGUE EVIDENCE CONVENTION

108. I am asked to examine the procedures that would be available to the US Court to obtain evidence located in the UK, if the proposed UK plaintiffs were to join the case. The most likely

route to obtaining evidence for the MDL from the UK is by the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters 1970 ("the Hague Evidence Convention").

109. The Hague Evidence Convention establishes a centralised mechanism for the provision of international judicial assistance in the taking of evidence abroad (in England, the Senior Master of the High Court). Chapter I of the Convention is concerned with the Letters of Request procedure and applies to Letters issued by the judicial authorities of a Contracting State in civil or commercial matters to obtain evidence intended for use in judicial proceedings, commenced or contemplated: Article 1. The request can cover a variety of forms of evidence, including oral testimony and the inspection of documents or other property (Article 3(1)) and is sent to a Central Authority designated for the purposes of the Convention in the country in which the evidence is to be taken.

110. The Hague Evidence Convention is implemented in the UK by the Evidence (Proceedings in Other Jurisdictions) Act 1975 ("the 1975 Act"). A key condition for the provision of assistance is in s.2(3): the English court may not order any steps to be taken unless they are steps which could be required to be taken by way of obtaining evidence for the purposes of civil proceedings in the English court.

111. The English courts have consistently held that they will not make orders for discovery which go beyond those permitted under English law. In this regard, it has been noted in several cases that the procedural rules of several US States and the US federal rules of civil procedure permit far wider forms of discovery (including "pre-trial discovery") which have no parallel in English law.[36]

112. In an important respect, the 1975 Act may leave a UK plaintiff litigating in a US court in a worse position than if he were litigating in an English court (to the extent that he needs to obtain documents or evidence in England). Under the 1975 Act, the court may not require a person to state what documents relevant to the foreign proceedings are in his possession, custody or power, or to produce any documents other than particular documents specified in the

[36] E.g., *Refco Capital Markets Ltd v Credit Suisse First Boston Ltd* [2001] EWCA Civ 1733.

court's order as being documents appearing to the court to be, or to be likely to be, in his possession, custody or power: s.2(3). The statutory reference to "*particular documents specified in the order*" is to be given a strict construction. It is not sufficient to refer to a class of documents; the order must specify with precision the documents are sought.

113. By contrast, a defendant to proceedings in England may be required to give disclosure of any and all documents which are or have been within his possession or control and which are relevant to any of the pleaded issues in the case.[37]

114. As a result of the detailed formal process under the Hague Evidence Convention (when compared to purely internal national rules) and the need to satisfy the standards of the requested State, it has been said that "*discovery under the Convention is often expensive and may yield uncertain results*".[38]

F. NOTIFICATION OF THE MDL PROCEEDINGS, AND THE HAGUE SERVICE CONVENTION

115. I am asked to examine the process and procedures that would be involved in giving UK class members service of the MDL proceedings under the Hague Service Convention. This is likely to be effected through the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters 1965 ("the Hague Service Convention").

116. As in the case of the Hague Evidence Convention, the Hague Service Convention adopts as its primary means of transmission a system of Central Authorities in each Contracting State, which bear the responsibility of arranging for the service of documents in the State.

117. In my experience, use of the Hague Service Convention between the English High Court and US courts can involve delays of up to four months and the process is noted for the costs and delays that can sometimes arise in it: e.g. *Marashen Ltd v Kenvett Ltd [2017]* EWHC 1706 (Ch), §50.

---

[37] Civil Procedure Rules, Part 31.

[38] *The Hague Convention: A Medium for International Discovery* (T. Abdollahi), The North Carolina Journal of International Law and Commercial Regulation, Vol. 4, No. 3 Spring 2015, p. 773.

118. The advantage of service under the Hague Service Convention is that, because of its formal conditions and use of a central authority, the legality of such service is normally not contested.

G. CONCLUSIONS

119. My views are stated under the headings set out above. Please do not hesitate to contact me with any queries arising from them.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed at London, United Kingdom, on the nineteenth day of May, 2020.

By: 

BRIAN KENNELLY Q.C., B.L.

19 May 2020

Blackstone Chambers

Temple

London EC4Y 9BW

Law Library

Four Courts

Dublin 8